A Message from the District Attorney

The Internet has become an essential part of our daily lives. People of all ages use the Internet for keeping in touch, sharing information and opinions, and pursuing common interests. Young people are especially active online, and are relying on the Internet to conduct educational research. However, their online activities may be exposing them to dangers such as predators who use the Internet to harm and exploit children. In addition, young people are utilizing new technologies such as MySpace which may not be familiar to their parents.

As Norfolk District Attorney and as a parent, I want to make sure that parents are aware of the risks involved in Internet use, and that we do everything we can to prevent Internet crimes before they happen.

- William R. Keating

"Prevent Internet crimes before they happen."

Internet Safety

A Guide for Parents

How to safeguard your children from online predators and exploitation

A Message from Norfolk County District Attorney Bill Keating

Warning Signs

Although children and teens place a high value on their privacy, it is important for parents to closely observe what their children are doing online. Parents should take note of attempts to conceal online activity, as they are usually a sign that the child is using the Internet inappropriately. The following are potential warning signs for dangerous online activity:

- When you enter a room, your child quickly clicks out of chat rooms/instant messages, changes the monitor's screen, or turns the computer off.
- Your child engages in Internet activity for long periods of time every day, often withdrawing from friends and family to be on the computer.
- Your child is using multiple screen names on the same account.
- Your child is receiving or making unexplained phone calls, whether to local, long distance, or 800 numbers.
- You note a sharp decrease in your child's academic performance.
- Your child demonstrates a sharp change in their behaviors and attitudes.
- Your child has made unauthorized use of a credit or debit card while online.
- Your child receives gifts or mail from an unknown or unexplained person.
- You find drug-related, racist, or pornographic material on your child's computer.
- Your child is reluctant to let you use his/her computer, check his/her email, or log on to his/her buddylist.

What to Do if Your Child is Victimized

Should any of these situations arise via the Internet or any online service, you should immediately contact your local police department, your District Attorney, the FBI, your Internet service provider, and the National Center for Missing and Exploited Children at (800) THE-LOST:

- Your child has been sexually solicited.
- Your child has receieved sexually-explicit images. These photos are often used by sexual predators to demonstrate that sexual relationships between adults and children are "normal."
- You, your child, or anyone receives child pornography.
- Your child or anyone in the household has been threatened.

Most importantly, keep the lines of communication open with your child. Remember that although your child may have gone against your wishes by speaking to someone online, the child is always the victim in these situations. Stay calm, and let your child know they are not at fault for being preyed upon.

The Internet is a worldwide, publicly-accessible network carrying information and services such as electronic mail, online chat, file transfer, and web pages on the World Wide Web. The Internet links us to a wealth of information and ideas, but also exposes children and adults to a number of risks. Parents and adults have a responsibility to protect children online and teach them basic safety rules concerning the Internet.

Basic Safety Rules

- Keep the computer in a common area, such as the kitchen, so you are able to easily monitor your child's activities.
- Become familiar with the Internet and services your child is using. Many children and teens use websites unfamiliar to parents, most notably MySpace and Facebook. These websites, which allow young people to create online profiles and post pictures, oftentimes contain inappropriate content (substance abuse, harassment, embarrassing pictures, etc.) and their level of detail makes it easy for predators to track down children. Parents should encourage their children not to create online profiles.
- Use filtering/blocking software, or parental control devices. Check with your Internet service provider for more information.
- Review the history folder in the browser of the computer with your child to review what websites he/she has accessed. Reluctance to share this information usually means inappropriate content has been viewed.

Electronic Mail (E-Mail)

E-Mail is a way of sending messages electronically from one computer to another. Children have access to E-Mail accounts through your Internet service provider (ISP), school-based networks, libraries, or online services (sometimes offering free accounts).

- Share a joint E-Mail account with your child, or know his/her password.
- Advise children not to open E-Mail from or respond to anyone they do not know. These messages could contain viruses or inappropriate content. Encourage your child to immediately delete these mesasges.
- Tell children not to respond to harassing or bothersome E-Mails. Advise them to share these messages with you immediately.
- Inform children that they are only to open attachments from people they know. Attachments may contain pornography, offensive material, or viruses.

"Become familiar with the Internet and services your child is using."

Chat Rooms

Chat rooms are online services allowing users to communicate with each other in "real-time." Because chat rooms are frequently used by predators preying on children, you may want to discourage any chat room use to avoid exposure to these risks.

- Talk to your child about the risks involved with chat rooms. Limit use to monitored chats or consider blocking chat entirely.
- Educate your child on common questions predators may ask. If a person asks your child if they are home alone, where the computer is or who has access to it, tell him/her to find you immediately.
- Tell your child never to begin a private chat with someone they do not know. Child predators almost always isolate their victims in private chats.
- If your child does participate in chats, advise them never to give out their real name (even their first) or other identifying information. Predators are adept at cataloguing these small details.

- Child predators oftentimes "lurk" in chat rooms without participating in conversation. This way, they may target a child who seems easily susceptible to private conversation.

Instant Messaging

Instant messaging refers to one-on-one conversations between two individuals on a "buddylist." Children may talk in real-time to one another, typically using America Online's service, AOL Instant Messenger (or AIM).

- Make passwords hard to guess using letters, numbers, and symbols. Tell your child never to give out his/her password to anyone but you.
- Monitor your child's buddylist and use of instant messenger. Excessive use (especially late at night) usually signals exclusive involvement with an individual.
- Enforce a time limit or only allow your child to be online during certain times of the day. While predators are always online, most incidents happen at night.

- Do not allow your child to create an online profile. A profile allows people to search for your child and gives extra information to predators.

"While predators are always online, most incidents happen at night."

- Tell your child never to send photographs of himself/herself or any individual over the Internet. These photos can not only aid predators in finding a child, but may also be unfavorably manipulated.
- Show your child how to utilize the "block" function to block anyone they do not know or who sends repeated messages. Contact your Internet service provider to become familiar with these control functions on your child's buddylist. Encourage your child to tell you if anyone makes them uncomfortable.

- If a child gets an instant message from someone he/she is not familiar with, tell him/her to quickly exit the screen. Many instant messenger applications (including AOL) have a feature which allows users to decline instant messages from people not on their buddylist.

Give your child a lesson on the unforgiving nature of cyberspace. Tell them never to send negative, threatening, or embarrassing messages. Everything said in cyberspace is there forever, for anyone to see.